6 February 2017

Joint Submission
Privacy International and the Italian Coalition for Civil Liberties
Consideration of the Sixth Periodic Report of Italy
Human Rights Committee 119th Session (6-29 March 2017)

1. Introduction

In its Concluding Observations of Italy's Fifth Periodic Report, adopted at its 2335th meeting, on 2 November 2005, the Human Rights Committee ("the Committee") called on Italy to "ensure that any restrictions on the right to privacy and family life are in accordance with the Covenant".[1]

In its Sixth Periodic Report, dating 8 October 2015, Italy brought to the attention of the Committee certain parliamentary debates surrounding amendments to its Criminal code and Code of Criminal Procedure. These amendments were aimed, as the Report describes them, "at striking a more satisfactory balance between the interests for security of the society... and, on the other hand, the individual fundamental rights, namely the right to respect for private and family life". Italy particularly noted to the Committee that any amendments adopted by Parliament surrounding covert surveillance techniques, will be "strictly limited".[2]

Privacy International and the Italian Coalition for Civil Liberties ("the organisations") wish to present to the Committee certain legal and political developments that have transpired in Italy since it submitted its State Report in October 2015. Particularly, the organisations wish

[1] Concluding Observations of the Human Rights Committee, Italy, U.N. Doc. CCPR/C/ITA/CO/5, para. 18 (24 April 2006).
[2] Sixth Periodic Reports of States before the Human Rights Committee, Italy, U.N. Doc. CCPR/C/ITA/6, para. 89 (16 November 2015) ("Considering the current debate on the possible revision (Bill 2798/C submitted by the Minister of Justice in February 2015) of the relevant norms aimed at striking a more satisfactory balance *between the interest for security of the society* (in this case the interest of criminal investigations) *and, on the other hand, the individual fundamental rights*, namely the right to respect for private and family life, the wiretapping of conversations and communications which results in forms of *covered surveillance techniques* placing obvious restrictions on the right to privacy and family life is *strictly limited* to specific given circumstances, envisaged by law.") Bill 2798/C, which has since been absorbed into Bill 2067/S, has been voted on by the Assembly on 27 September 2016 but has not yet been adopted.

to underline to the Committee its ongoing concern with Italian security agencies' hacking capabilities and intelligence sharing arrangement, with Italian data retention procedures, and its export control regime as it relates to its robust private surveillance technologies sector.

2. Hacking Powers

Article 266(1) of the Italian Code of Criminal Procedure allows for the "interception of conversations or communications" in proceedings relating to a list of predefined serious crimes. Article 266-bis expands the surveillance powers authorized to include "interception of the flow of communications related to computerized systems". Nonetheless, Art. 266(2) prohibits any interception carried out in a home or dwelling, or in another building or structure of private ownership, unless there is reason to believe that criminal activity has taken or is taking place within that building.

Given the qualifier in Article 266(2), it was assumed that law enforcement may not conduct remote hacking of electronic devices (including laptops, smartphones, and tablets) using covert malicious software. This is because such hacking would grant the authorities unrestricted and complete access and control over the device in question. The hacked device thus becomes the perfect spy, continuously and unabatedly sensing and monitoring the target's environment, to the whims of its controller.[3] This includes, amongst other things: (1) the capturing of all incoming or outgoing data traffic (*e.g.* browsing history, email usage, content of communications, geospatial location, text messages, and photos); (2) the ability to switch on and off the microphone and camera of a device, without its owner's knowledge; (3) searching the hard drive and making copies of all or part of the computer system's memory units; (4) deciphering everything that is typed on the keyboard, using key-loggers, and collecting anything that is seen on the screen, by taking screenshots, regardless of whether the owner had used encryption software.[4]

Attempts by the legislator to amend Article 266 of the Code of Criminal Procedure to explicitly authorize remote hacking of devices, has so far not materialized. The original draft of the Italian Anti-Terrorism Decree,[5] adopted by the Senate on 15 April 2015, included a provision which would have amended Art. 266 of the Code of Criminal Procedure of Italy by introducing the possibility of using intrusive software to remotely acquire data and communications of computer systems.[6] Due to public pressure the law that was eventually adopted excluded any reference to such hacking powers.[7] Subsequent attempts, including Bills 3470/C and 3762/C which both proposed amendments to interception of electronic communications from a computer system, did not advance in Parliament. Nonetheless, two recent developments have brought remote and covert hacking by Italian authorities back into the fold.

---

[3] Corte di Cassazione, Sezioni Unite, Sentenza 1 Iuglio 2016, n. 26889, Pres. Canzio, Conduct of Case, para. 2 (referring to a "real environmental interception", vera e propria intercettazione ambientale).
[4] *Id*., Reasons for the Decision, para. 2.
[5] Decreto-Legge 18 febbraio 2015, n. 7, Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonché proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione.
[6] The amendment would have inserted the words: "including through the use of tools or computer programs for the acquisition of remote communications and data in a computer system".
[7] For further reading see, Italy: Anti-Terrorism Decree to Strengthen Government Surveillance, EDRi (22 April 2015), *available at* https://edri.org/italy-anti-terrorism-decree-strengthen-government-surveillance/.

The Supreme Court of Italy (*Corte Suprema di Cassazione*) ruled on 1 July 2016 that remote and covert hacking was lawful even within the limited bounds of Article 266.[8] The Court particularly noted that at the time of "authorizing an interception to be carried out by means of computer sensor installed on a portable device, the judge can not foresee and pre-determine the private dwellings in which the electronic device will be introduced, resulting in inability to exercise adequate control about the actual compliance with the legislation."[9] Nonetheless, given the threats posed to society by "structured criminal organizations that have sophisticated technologies and significant financial resources", and in particular global terrorist organizations, the "current legislation as well as the constitutional principles" must "adapt effectively".[10] The Court further concluded that such hacking would also be in compliance with Italy's obligations under Article 8 of the European Convention of Human Rights and Fundamental Freedoms.

A private draft bill, submitted by MP Stefano Quintarelli, titled "Rules Governing the Use of Government Trojan with Respect For Individual Rights", also known as the "Trojan Bill", is currently pending before the Justice Committee of the Italian Parliament.[11] The bill calls for amending Article 266 to reflect the Court's judgment, as well as establish a more robust system for authorizing remote and covert hacking.

The Organisations strongly oppose hacking as a tool for surveillance, given both the pervasiveness of the interference to privacy and the consequences it might have on the security and integrity of communications systems. Of particular concern is the fact that hacking, including as reflected in the bill, goes beyond the mere warrant-based collection of necessary intelligence for the purposes of conducting investigations over the most serious crimes, and involves complete access to and control over electronic devices with no limitations or qualifiers. In other words, a single warrant from a judge would suffice to conduct an array of intelligence activities ranging from passive copying of information to offensive manipulation with the devices' data and functions. This stands in contrary to longstanding position of the Committee that any surveillance activity requires a warrant.[12]

Moreover, given the type of control in question and the kind of surveillance envisioned by the bill, this is completely disproportioned. As was further explained by U.N. Special Rapporteur on Freedom of Expression:

---

[8] Corte di Cassazione, *supra* note 3, Reasons for the Decision, para. 11 ("limited exclusively to proceedings relating to offences of organized crimes, the Court allows the real-time interception of conversations or communications by installing a "computerized sensor" in portable electronic devices (e.g. personal computer, tablet, smartphone, etc.) also in private homes under Art. 614 of the Code of Criminal Procedure, even if those dwelling are not identified in the warrant or if it is not determined that they were used to conduct criminal activity") (in the original Italian "Limitatamente ai procedimenti per delitti di criminalità organizzata, è consentita l'intercettazione di conversazioni o comunicazioni tra presenti mediante l'installazione di un captatore informatico in dispositivi elettronici portatili (ad es., personal computer, tablet, smartphone, ecc.) - anche nei luoghi di privata dimora ex art. 614 c.p., pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa").

[9] *Id*., Reasons for Decision, para. 6.

[10] *Id*., Reasons for Decision, para. 10.1.

[11] Prposta di Legge, Disciplina dell'uso dei Captatori legali nel rispetto delle garanzie individuali. The full Italian bill, and its summary in English are both available at http://www.civicieinnovatori.it/wp-content/uploads/2017/02/Sintesi-PDL-captatori-EN.pdf.

[12] *See e.g.*, Concluding Observations on the Fourth Periodic Report of the Republic of Korea, Human Rights Committee, U.N. Doc. CCPR/C/KOR/CO/4, para. 43 (3 December 2015).

> "Offensive intrusion software such as Trojans, or mass interception capabilities, constitute such serious challenges to traditional notions of surveillance that they cannot be reconciled with existing laws on surveillance and access to private information. There are not just new methods for conducting surveillance; they are new forms of surveillance. From a human rights perspective, the use of such technologies is extremely disturbing. Trojans, for example, not only enable a State to access devices, but also enable them to alter – inadvertently or purposefully – the information contained therein. This threatens not only the right to privacy but also procedural fairness rights with respect to the use of such evidence in legal proceedings."[13]

In recent years we have seen a rise in over-reliance by law enforcement and intelligence agencies around the world of various tools for remote and covert hacking through intrusive software. The Italian authorities have been employing hacking powers, without explicit statutory authorization or clearly defined safeguards from abuse for years.[14] While the attempts to regulate hacking powers through primary legislation contribute to exposing the practice and allow for greater public scrutiny over it, they nonetheless also illustrate the difficulties in reconciling state hacking capabilities with international human rights law. This poses an opportunity for the Committee to elaborate on how state hacking may violate the right to privacy as enshrined in Article 17 of the ICCPR.

3. Intelligence Sharing

According to the revelations made by former NSA contractor Edward Snowden, Italy is considered a Senior SIGINT partner in Europe (SSEUR) as part of its membership within the "14-Eyes. This network was established for the purpose of coordinating the exchange of communications intelligence amongst all fourteen States,[15] and the Committee has already expressed its concerns about the surveillance activities of some of these states, including in the context of mass surveillance.[16] Italy is additionally a party to a number of other intelligence sharing arrangements including the NATO Advisory Committee on Special Intelligence (NACSI) and the European "Club de Berne".[17] Italy has in the past expressed

[13] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/23/40, para. 62 (17 April 2013).

[14] For further reading *see* Carola Frediani, *Intercettazioni col trojan, ecco la proposta di legge*, LA STAMPA (31 January 2017), *available at* http://www.lastampa.it/2017/01/31/italia/cronache/intercettazioni-col-trojan-ecco-la-proposta-di-legge-MP8BJ2PB0jCwMt84ofRSlM/pagina.html (noting that MP Quintarelli has said in a press conference that: "Today these tools are used without a system of guarantees and we do not even know how many people are subjected [to such measures of control]").

[15] Ewen MacAskill and James Ball, *Portrait of the NSA: No Detail too Small in Quest for Total Surveillance*, THE GUARDIAN (2 November 2013).

[16] *See e.g.*, Concluding Observations of the Fourth Periodic Report of the United States of America, Human Rights Committee, U.N. Doc. CCPR/C/USA/CO/4, para. 22 (23 April 2014); Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7, para. 24 (17 August 2015); Concluding observations on the fifth periodic report of France, Human Rights Committee, U.N. Doc. CCPR/C/FRA/CO/5, para. 12 (17 August 2015); Concluding Observations on the Sixth Periodic Report of Canada, Human Rights Committee, U.N. Doc CCPR/C/CAN/CO/6, para. 10 (13 August 2015); Concluding Observations on the Sixth Periodic Report of Denmark, Human Rights Committee, U.N. Doc. CCPR/C/DNK/CO/6, para. 27 (15 August 2016).

[17] *See generally* Five Eyes, 9-Eyes, and many more, electrospaces.net (22 January 2014), *available at* http://electrospaces.blogspot.co.uk/2013/11/five-eyes-9-eyes-and-many-more.html.

interest in ensuring greater intelligence sharing and accessibility to datasets amongst European Partners.[18]

In this regard, concerns are heightened considering Italy's engagement in intelligence sharing with Governments which are known for their serious violations of international human rights law, including the ICCPR. For example, in February 2016 Italy signed an agreement with the Nigerian Government on intelligence sharing[19]; and reportedly the director of the Italian intelligence were in contact, in late 2016, with the Syrian Government to discuss the possibility of intelligence sharing arrangements.[20]

Combined these reports raise serious concerns about Italy's potential complicity in unlawful surveillance and interferences with individuals' privacy. Lack of legal safeguards and effective oversight in relation to intelligence sharing had already been a concern of the Committee, as expressed for example in the concluding observations on Sweden.[21]

4. Data Retention

The Italian Personal Data Protection Code establishes in Section 123(2) that providers "shall be allowed to process traffic data that are strictly necessary for contracting parties' billing and interconnection payments for a period not in excess of six months". Section 132 of the Act establishes an exception to that rule for purposes of crime prevention, noting that:

> "telephone traffic data shall be retained by the provider for twenty-four months as from the date of the communication with a view to detecting and suppressing criminal offences, whereas electronic communications traffic data, except for the contents of communications, shall be retained by the provider for twelve months as from the date of the communication with a view to the same purposes. The data related to unsuccessful calls that are processed on a provisional basis by the providers of publicly available electronic communications services or a public communications network shall be retained for thirty days."[22]

Such data may then be acquired from the provider by means of an order issued by the public prosecutor.

In connection with investigations of serious crime, the Anti-Terrorism Decree,[23] as was amended on 24 February by a subsequent decree ("Milleproroghe" decree),[24] compels

---

[18] *See e.g.*, Zeeke Turner, *Germany's Angela Merkel Calls for More Sharing of Intelligence Information in EU*, WSJ (22 August 2016), *available at* https://www.wsj.com/articles/germanys-angela-merkel-calls-for-more-sharing-of-intelligence-information-in-eu-1471886210

[19] *See* Mohammed Abubakar, *Nigeria, Italy Pledge to Strengthen Bilateral Relations*, THE GUARDIAN (2 February 2016), *available at* http://guardian.ng/news/nigeria-italy-to-pledge-to-strengthen-bilateral-relations/.

[20] *See Syria Regime Campaigns to Mend Relations with EU*, GULF NEWS (6 July 2016), *available at* http://gulfnews.com/news/mena/syria/syria-regime-campaigns-to-mend-relations-with-eu-1.1858261.

[21] Concluding Observations on the Seventh Periodic Report of Sweden, Human Rights Committee, U.N. Doc. CCPR/C/SWE/CO/7, paras. 36-37 (28 April 2016); *See also*, Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7, para. 24 (17 August 2015); Concluding Observations on the Sixth Periodic Report of Canada, Human Rights Committee, U.N. Doc CCPR/C/CAN/CO/6 (13 August 2015).

[22] Codice in materia di protezione dei dati personali, D.Lgs. 30/06/2003 n. 196 ("Codice Privacy") (Personal Data Protection Code, Legislative Decree no. 196, Section 132 (Traffic Data Retention for Other Purposes) (30 June 2003)).

[23] Decreto-Legge 18 febbraio 2015, n. 7, *supra* note 5, at 4-bis.

telecom operators to retain already collected data until 30 June 2017 and beyond the times allocated in the Personal Data Protection Code. Retention terms under Article 132 will then be either reinstated or prolonged even further, as the Government has not yet indicated its intentions.[25]

The Committee has already recommended that State Parties should "refrain from imposing mandatory retention of data by third parties".[26]

This recommendation is further reinforced by the recent judgment of the Court of Justice of the European Union in the Tele2/Watson Case. Firstly, that judgment reaffirmed and expanded on the invasive nature of metadata collection in the context of the right to privacy:

> "That data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular that data provides the means... of *establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications."* (emphasis added).[27]

Secondly, with regards to the Governments' claims that the indiscriminate retention of data for the purposes of fighting terrorism, the Court noted that:

> "effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight."[28]

Finally, as relating to access to retained data the Court took the position that:

> "it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an

---

[24] Decreto-Legge 30 dicembre 2016, n. 244, Proroga e definizione di termini.

[25] For further reading, *see* The Data Retention Saga Continues: European Court of Justice and EU Member States Scrutinize National Data Retention Laws, Jones Day (August 2016), *available at* http://www.jonesday.com/the-data-retention-saga-continues-european-court-of-justice-and-eu-member-states-scrutinize-national-data-retention-laws-08-11-2016/.

[26] Concluding Observations of the Fourth Periodic Report of the United States of America, Human Rights Committee, U.N. Doc. CCPR/C/USA/CO/4, para. 22 (23 April 2014); *See also* Concluding Observations on the Initial Report of South Africa, Human Rights Committee, U.N. Doc. CCPR/C/ZAF/CO/1, para. 43 (27 April 2016) ("The State Party should... consider revoking or limiting the requirement for mandatory retention of data by third parties...").

[27] Tele2 Sverige AB v. Post- Och telestyrelsen (C-203/15); Secretary of State for the Home Department v. Tom Watson et. al. (C-698/16), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment, para. 99 (21 December 2016). This position is in line with the Committee's approach to indiscriminate gathering of metada as reflected for example in Concluding Observations on the Seventh Periodic Report of Poland, Human Rights Committee, U.N. Doc. CCPR/C/POL/CO/7 (4 November 2016).

[28] *Id*., at para. 103.

> independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime".[29]

The Italian law imposes on Telecom providers obligations to engage in indiscriminate data retention, in violation of Article 17 of the ICCPR and clearly in stark contradiction with the jurisprudence of the CJEU. Moreover, the temporal limitations that were introduced in the Personal Data Protection Code have been cast aside through Governmental decrees, allowing for retention of data for even greater periods. That in itself constitutes a violation of the right to privacy. Even further, access to such data by the authorities is not subject to authorization from a judicial authority.

5. Italy's Private Surveillance Sector

Italy is a significant European hub for the exporting of defence, surveillance and arms equipment and technologies. There are currently 18 Italian companies featured in Privacy International Surveillance Industry Index (SII), an online database which aims to track companies developing and selling electronic surveillance technology. In addition to having a large defence and security sector generally, the Italian surveillance industry has been driven by domestic demand to fight organised crime.[30] The organisations are particularly concerned about Italy's surveillance sector's dealings with authoritarian governments with a poor human rights record. In particular, we wish to bring to the Committee's attention recent developments surrounding two such companies, which exemplify some of the existing structural inadequacies of the Italian export control regime.

Hacking Team

Much of the information we have on Italian surveillance exports relates to Hacking Team, a developer and seller of intrusion technology based in Milan. The company's "Remote Control Systems" (RCS) enables government law enforcement and intelligence agencies to monitor the communications and data of targets' digital devices, view their encrypted files and emails, record Skype and other Voice over IP communications, identify their geographical location, and remotely activate microphones and camera on target computers.[31] Hacking Team has attracted the most attention among surveillance companies as a result of their internal systems being hacked in 2015 and subsequent revelations that they had exported to a range of authoritarian countries, including in Sudan, Ethiopia, Egypt, Turkey, Bahrain, Venezuela, and Saudi Arabia.[32] In September 2016, a United Nations Panel of Experts on the Sudan, which monitors the enforcement of sanctions in Darfur and which had been investigating evidence that Hacking Team's equipment was in use in Sudan, found that "Hacking Team certainly obstructed the work of the Panel by consistently and deliberately

[29] *Id*., at para. 120.
[30] For further reading, *see* The Global Surveillance Industry, Privacy International (July 2016), *available at* https://privacyinternational.org/sites/default/files/global_surveillance.pdf.
[31] *See Enemies of the Internet: Hacking Team*, Reporters Without Borders (17 February 2016), *available at* http://surveillance.rsf.org/en/hacking-team/.
[32] Eric King, *Surveillance Company Hacking Team Exposed*, Privacy International (6 July 2015), *available at* https://www.privacyinternational.org/node/618.

failing to provide the specific information at its disposal, as requested by the Panel, and thus failed to comply with paragraph 22 of [U.N. Security Council] resolution 2200".[33]

Hacking Team RCS spyware has reportedly been used to target, amongst others, award winning Moroccan media outlet Mamfakinch,[34] the UAE human rights activist Ahmed Mansoor,[35] and Ethiopian journalists in the Washington DC area.[36]

The Italian Ministry of Economic Development first imposed a "catch-all" licensing obligation on Hacking Team's sales in 2014, as recommended by an earlier letter to the Ministry from the Organisations,[37] but subsequently granted the company a global export license in 2015 which allowed the company to export around the world with minimal oversight. Its global licence was later revoked in 2016, which meant that the company would have to apply for individual licenses to export outside of the EU.[38] At the time of writing, it has been reported that decisions by the Ministry on granting individual licenses to Hacking Team have been frozen.[39] On 15 July 2016, the Regional Administrative Court of Lazio rejected a request by Hacking Team for an injunction against the revocation. That decision has been appealed by Hacking Team and is pending before the State Council.[40]

Area SpA

Area SpA was established in 1996 in the province of Varese in Lombardy. The company develops and markets monitoring centres used to intercept, store, and analyse voice and internet traffic. These centres not only allow for the collection of data but its comparative analysis and processing. The company claims to have exported 300 of these systems around the world.[41] In 2009 Area SpA signed a contract with the Assad government to install a monitoring centre in Syria. As the regime began its violent crackdown on democratic protests, the Italian authorities issued a "catch all" export requirement on the company in

[33] Letter from Issa Maraut, Panel of Experts on the Sudan Established under Resolution 1591, to Mr. Sebastiano Cardi, Permeant Representative of Italy to the United Nations, U.N. Doc. S/AC.47/2015/PE/OC.23 (18 March 2015).

[34] For further reading, *see* Ryan Gallagher, How Government-Grade Spy Tech Used A Fake Scandal To Dupe Journalists, Slate (20 August 2012) *available at* http://www.slate.com/blogs/future_tense/2012/08/20/moroccan_website_mamfakinch_targeted_by_government_grade_spyware_from_hacking_team_.html

[35] *See* Backdoors are Forever: Hacking Team and the Targeting of Dissent?, Citizen Lab (10 October 2012) *available at* https://citizenlab.org/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/.

[36] For further reading, *see* Bill Marczak et. al., *Mapping Hacking Team's "Untraceable" Spyware*, Citizen Lab (17 February 2014), *available at* https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/.

[37] Under a provision in the Italian law, known as "catch all", the Government may impose an obligation on a company to apply for individual licences per each sale it makes, this allows for better control on the part of the authorities to ensure that no equipment is exported if there is a clear risk to human rights.

[38] For further reading, *see* Edin Omanovic, Hacking Team's Global Licence Revoked by the Italian Export Authorities, Privacy International (8 April 2016), *available at* https://www.privacyinternational.org/node/826.

[39] *See* Giulio Simeone, *Hacking Team. "Motivazione inadeguata": il Consiglio di Stato contraddice il Mise sulla revoca dell'autorizzazione all'export*, il Fatto Quotidiano (2 November 2016), *available at* http://www.ilfattoquotidiano.it/2016/11/02/hacking-team-motivazione-inadeguata-il-consiglio-di-stato-contraddice-il-mise-sulla-revoca-dellautorizzazione-allexport/3163585/.

[40] *Ibid*.

[41] *See* Area SpA Website, Products, *available at* http://www.area.it/?page_id=28 (last accessed: 31 January 2017).

September 2012.[42] In late 2015 Italian and international media reported that the offices of Area SpA had been raided by Italian law enforcement, for unspecified reasons.[43]

Another media report, published in June 2016, states that Area SpA had been granted an export license by Ministry of Electronic Development to export internet traffic surveillance technologies to the Technical Research Department (TRD) of the Egyptian National Defence Council for 3.1 million dollars.[44] The TRD, is a little known and shadowy branch of the Egyptian intelligence apparatus. A link has been drawn between the purchase of surveillance technologies by the TRD and a pattern of political repression and curtailment of press freedoms.[45] The authorisation was granted as agencies of the EU, the United Nations and NGOs were all were reporting concerns about the deteriorating human rights situation in Egypt.[46]

The Organizations and the Hermes Center for Transparency and Digital Human Rights, sent a letter to the Italian export authorities in January 2017 asking for assurances about the report and whether the Ministry would consider revoking the authorisation. On 23 January 2017 the Ministry of Economic Development published an official statement noting that a review process began in July 2016 and that on the basis of which Area SpA's license was suspended, and that it will be revoked in the next meeting of the Special Advisory Committee to the Ministry.[47]

Areas of Concern

Both examples elucidate core limitations surrounding the ability to scrutinize Italian regulation of its surveillance sector. Two points are of particular concern.

First, the Italian Export Authorities do not publish, on a routine basis, export licencing information, or other data pertaining to their determinations and decision making. Transparency on export licensing is essential to provide the public and Italian Parliament with oversight and confidence in the export licensing system. Moreover, as companies themselves refuse to disclose any information as to their trade agreements or licencing, without export licensing data there is little opportunity for the parliament or public to hold

[42] *See* Trevor Timm, S*py Tech Companies & Their Authoritarian Customers, Part II: Trovicor and Area SpA*, EFF (21 February 2012), *available at* https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-ii-trovicor-and-area-spa.

[43] Lorenzo Franceschi Bicchierai, Italian Cops Raid Surveillance Tech Company Accused of Selling Spy Gear to Syria, MOTHERBOARD (1 December 2016), *available at* http://motherboard.vice.com/read/italian-cops-raid-surveillance-tech-company-area-spa-selling-spy-gear-to-syria.

[44] For further reading, *see* Carola Frediani, L'Italia esporterà software di sorveglianza in Egitto, LA STAMPA (28 June 2016), *available at* http://www.lastampa.it/2016/06/28/italia/litalia-esporter-software-di-sorveglianza-in-egitto-11iR9uYFcPpkP9PebyHdwM/pagina.html.

[45] For more information about the TRD, *see* The President's Men, Privacy International (February 2016), *available at* https://privacyinternational.org/sites/default/files/egypt_reportEnglish.pdf.

[46] For further reading see, Italian Authorities Urged to Act Following Reports of Internet Surveillance System Being Exported to Egypt, Privacy International (23 January 2016), *available at* https://medium.com/privacy-international/italian-authorities-urged-to-act-following-reports-of-internet-surveillance-system-being-exported-c1defc3afe46#.se7pzltxy.

[47] Già sospesa autorizzazione a AREA per esportazione in Egitto sistema monitoraggio comunicazioni, Ministero Dello Sviluppo Economico (23 January 2017), *available at* http://www.sviluppoeconomico.gov.it/index.php/it/per-i-media/comunicati-stampa/2035887-gia-sospesa-autorizzazione-a-area-per-esportazione-in-egitto-sistema-monitoraggio-comunicazioni.

government decisions to account for its decisions in the sphere of ensuring compliance with human rights obligations. Challenges to Italy's surveillance industry are therefore largely dependent upon investigative reporting by journalists and researchers, and leaks, which are insufficient as an accountability scheme.

Second, and directly related to the point above, while the eventual actions taken by the Italian Ministry to suspend Hacking Team's global license and Area SpA's license to Egypt are to be commended, there still exists an urgent need to improve the current regulatory system.

The duty to respect and to ensure that individuals enjoy their civil and political rights, enshrined in ICCPR Article 2(1), entails a due diligence obligation on the part of the State vis-à-vis the activities of private companies in its jurisdiction. The United Nations General Assembly has further reaffirmed this position, as it relates to the right to privacy, as recently as 19 December 2016, concluding that:

> "business enterprises have a responsibility to respect human rights and that States must protect against human rights abuses, including of the right to privacy, within their territory and/or jurisdiction by third parties, including business enterprises, as set out in the Guiding Principles on business and Human rights: Implementing the United Nations "Protect, Respect and Remedy" Framework and in accordance with applicable laws and other international principles"[48]

Italy is thus under an obligation to conduct routine reviews of its licencing arrangements, and act with no hesitation to prevent abuses before they occur. Assessment criteria used by the Italian authorities to assess applications by companies for export licenses should ensure that no exports are authorised if they risk facilitating human rights violations. Within their assessment criteria for licenses for surveillance technology, the Italian authorities should, among numerous other factors, assess the legal framework governing the use of the technology in the destination country, the human rights record of the proposed end-user, and the safeguards and oversight procedures in place for the use of surveillance powers.

6. Recommendations

Based on the above observations, the organisations propose the following recommendations to the Italian Government:

- The Government should immediately cease any acts of surveillance conducted by means of hacking to electronic devices through intrusive software, and launch a thorough assessment based on international human rights law to establish if hacking-based surveillance powers are compatible Article 17 of the Covenant and in particular with the principles of legality, necessity and proportionality as interpreted by the Committee.

[48] U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/71/199 (19 December 2016).

- The Government should review the practice of intelligence sharing with foreign agencies to ensure its compliance with the right to privacy, under Article 17 of the Covenant. In particular, the Government should aim to ensure greater transparency surrounding these intelligence sharing arrangements, subject such arrangements to primary legislation and parliamentary scrutiny, and establish independent oversight mechanisms to prevent abuses in the course of these arrangements and to ensure that individuals have access to effective remedies.

- The Government should refrain from imposing on telecommunication companies and third parties indiscriminate obligations to retain communications data, and should review its laws to ensure that any such obligations or requests to access such data are subject to tests of necessity and proportionality and authorized by judicial body.

- The Government should strengthen the regulation of the export of surveillance technologies by private companies registered or licenced in Italy. The Government should prevent the export of surveillance technologies where there is a risk they will be used to undermine human rights, and should ensure that information surrounding its exports is made available to Parliament and the general public to foster greater accountability.